CLAIMS

1. A communication apparatus for communicating with a server apparatus based on a server certificate that indicates validity of said server apparatus, comprising:

a revocation number obtainment unit operable to obtain a revocation number from a repository apparatus storing said revocation number that is information serving as a criterion for judging validity of the server certificate;

a revocation number storage unit operable to store the obtained revocation number;

an identification number reading unit operable to read out, from the server certificate, an identification number used to identify said server certificate;

a certificate judgment unit operable to judge the validity of the server certificate by comparing the read-out identification number with the revocation number stored by the revocation number storage unit; and

a communication control unit operable to establish a communication with the server apparatus when the server certificate is judged to be valid, and operable not to establish a communication with the server apparatus when the server certificate is judged to be invalid.

2. The communication apparatus according to Claim 1,

wherein the certificate judgment unit judges that the server certificate is valid, when the identification number is equal to or larger than the revocation number.

3. The communication apparatus according to Claim 1, further comprising a revocation number judgment unit operable to judge validity of the revocation number,

wherein the certificate judgment unit judges the validity of the server certificate by use of the revocation number, when the revocation number judgment unit judges that the revocation number is valid.

4. The communication apparatus according to Claim 3,

wherein the revocation number judgment unit judges the validity of the revocation number by comparing an identification number of a repository certificate indicating validity of the repository apparatus with the revocation number stored by the revocation number storage unit.

5. The communication apparatus according to Claim 4,

wherein the revocation number judgment unit judges that the repository apparatus is valid, when the identification number of the repository certificate is equal to or larger than the revocation number stored by the revocation number storage unit.

6. The communication apparatus according to Claim 3,

wherein the revocation number judgment unit judges the validity of the revocation number obtained by the revocation number obtainment unit by comparing said revocation number obtained by the revocation number obtainment unit with the revocation number stored by the revocation number storage unit.

7. The communication apparatus according to Claim 6,

wherein the revocation number judgment unit judges that the revocation number obtained by the revocation number obtainment unit is valid, when said obtained revocation number is equal to or larger than the revocation number stored by the revocation number storage unit.

8. A certificate issuing apparatus for issuing a server certificate indicating validity of a server apparatus, comprising:

a revocation number storage unit operable to store a revocation number that is information serving as a criterion for judging validity of the server certificate; and

an issuing unit operable to issue a new server certificate,

wherein the issuing unit issues the new server certificate that includes an identification number indicating a value which is equal to or larger than the revocation number stored by the revocation number storage unit.

9. The certificate issuing apparatus according to Claim 8, further comprising a revocation number update unit operable to update the revocation number stored by the revocation number storage unit to a number larger than an identification number of a server certificate to be revoked, when notified of said identification number of the server certificate to be revoked.

10. The certificate issuing apparatus according to Claim 9,

wherein the issuing unit issues the new server certificate for a server apparatus with a server certificate that is assigned an identification number smaller than the updated revocation number, in the case where the revocation number update unit updates the revocation number stored by the revocation number storage unit.

11. The certificate issuing apparatus according to Claim 8, further comprising a revocation number update unit operable to specify an identification number of a server certificate, an expiration date of which is approaching, and update the revocation number stored by the revocation number storage unit to a number larger than said identification number.

12. The certificate issuing apparatus according to Claim 11,

wherein the issuing unit issues the new server certificate for a server apparatus with a server certificate that is assigned an identification number smaller than the updated revocation number, in the case where the revocation number update unit updates the revocation number stored by the revocation number storage unit.

13. A communication system comprising a server apparatus, a certificate issuing apparatus for issuing a server certificate indicating validity of the server apparatus, and a communication apparatus for communicating with the server apparatus based on said server certificate,

wherein the certificate issuing apparatus includes:

a first revocation number storage unit operable to store a revocation number that is information serving as a criterion for judging validity of the server certificate; and

an issuing unit operable to issue a new server certificate,

wherein the issuing unit issues the new server certificate that includes an identification number indicating a value which is equal to or larger than the revocation number stored by the first revocation number storage unit, and

the communication apparatus includes:

a revocation number obtainment unit operable to obtain a revocation number from a repository apparatus storing said revocation number that is information serving as a criterion for judging the validity of the server certificate;

a second revocation number storage unit operable to store the obtained revocation number;

an identification number reading unit operable to read out, from the server certificate, an identification number used to identify said server certificate;

a certificate judgment unit operable to judge the validity of

the server certificate by comparing the read-out identification number with the revocation number stored by the second revocation number storage unit; and

a communication control unit operable to establish a communication with the server apparatus when the server certificate is judged to be valid, and operable not to establish a communication with the server apparatus when the server certificate is judged to be invalid.

14. A communication method for carrying out a communication with a server apparatus based on a server certificate indicating validity of said server apparatus, comprising:

a revocation number obtainment step of obtaining a revocation number from a repository apparatus storing said revocation number that is information serving as a criterion for judging validity of the server certificate;

a revocation number storage step of storing the obtained revocation number into a recording unit;

an identification number reading step of reading out, from the server certificate, an identification number used to identify said server certificate;

a certificate judgment step of judging the validity of the server certificate by comparing the read-out identification number with the revocation number stored by the recording unit; and

a communication control step of establishing a communication with the server apparatus when the server certificate is judged to be valid, and of not establishing a communication with the server apparatus when the server certificate is judged to be invalid.

15. A certificate issuing method for issuing a server certificate indicating validity of a server apparatus, comprising:

a revocation number storage step of storing, into a recording unit, a revocation number that is information serving as a criterion for judging validity of the server certificate; and

an issuing step of issuing a new server certificate,

wherein in the issuing step, the new server certificate that includes an identification number is issued, the identification number indicating a value which is equal to or larger than the revocation number stored by the recording unit.

16. A program for a communication apparatus that communicates with a server apparatus based on a server certificate indicating validity of said server apparatus, the program causing a computer to execute the following steps:

a revocation number obtainment step of obtaining a revocation number from a repository apparatus storing said revocation number that is information serving as a criterion for judging validity of the server certificate;

a revocation number storage step of storing the obtained revocation number into a recording unit;

an identification number reading step of reading out, from the server certificate, an identification number used to identify said server certificate;

a certificate judgment step of judging the validity of the server certificate by comparing the read-out identification number with the revocation number stored by the recording unit; and

a communication control step of establishing a communication with the server apparatus when the server certificate is judged to be valid, and of not establishing a communication with the server apparatus when the server certificate is judged to be invalid.

17. A program for a certificate issuing apparatus that issues a

server certificate indicating validity of a server apparatus, the program causing a computer to execute the following steps:

a revocation number storage step of storing, into a recording unit, a revocation number that is information serving as a criterion for judging validity of the server certificate; and

an issuing step of issuing a new server certificate,

wherein in the issuing step, the new server certificate that includes an identification number is issued, the identification number indicating a value which is equal to or larger than the revocation number stored by the recording unit.